<table>
<thead>
<tr>
<th>Partner Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Partner Name</td>
</tr>
<tr>
<td>Website</td>
</tr>
<tr>
<td>Product Name</td>
</tr>
<tr>
<td>Partner Contact</td>
</tr>
<tr>
<td>Support Contact</td>
</tr>
<tr>
<td>Product Description</td>
</tr>
</tbody>
</table>
Use Cases for Integration with the Palo Alto Networks Security Operating Platform

Challenge: Tracking and automating security for dynamic workloads is complex, hard to manage, and difficult to deploy

- Workloads are dynamic: IP addresses can change as workloads move (live-migrate) across data centers and clouds
- Dynamic changes to workload policies can be cumbersome and hard to administer
- Workloads can be spun up or down

Solution

- Illumio helps you to intelligently tag and push real-time context across workloads into Panorama and Palo Alto Networks firewalls
- Automate Dynamic Address Group (DAG) policy changes to reduce risk and implement effective workload controls

Table 1: Integration Details by Product

<table>
<thead>
<tr>
<th>Palo Alto Networks Product</th>
<th>Integration Status</th>
<th>Palo Alto Networks Versions Tested</th>
<th>Illumio Versions Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoFocus™</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cortex XDR™</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next-Generation Firewall</td>
<td>Illumio: Testing complete</td>
<td>PAN-OS® 8.1.9 &amp; 9.1</td>
<td>PCE 20.1, PCE 19.3, PCE 19.1, PCE 18.2</td>
</tr>
<tr>
<td>Panorama™</td>
<td>Illumio: Testing complete</td>
<td>PAN-OS® 9.1</td>
<td>PCE 20.1, PCE 19.3, PCE 19.1, PCE 18.2</td>
</tr>
<tr>
<td>Prisma™ Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prisma™ Cloud Compute</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prisma™ Cloud Enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prisma™ SaaS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM-Series</td>
<td>Illumio: Testing complete</td>
<td>PAN-OS® 8.1.9 &amp; 9.1</td>
<td>PCE 20.1, PCE 19.3, PCE 19.1, PCE 18.2</td>
</tr>
<tr>
<td>WildFire®</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Integration use cases for dynamically registering IP address and tags on Palo Alto Networks Panorama as well as physical and virtual Palo Alto Networks Next-Generation Firewalls (NGFWs):

- Register new workload: When a workload is paired with Illumio’s Policy Compute Engine (PCE), the corresponding IP address and tags are dynamically registered.
- Workload label change: When label(s) associated with a workload changes on Illumio’s PCE, corresponding tags are dynamically registered.
- Workload IP address change: When a workload IP address changes, a new IP address is dynamically registered and the old IP address unregistered.
- Workload termination: When a workload is terminated, the corresponding IP address is unregistered.

Integration Benefits

Comprehensive Application and Workload Visibility
- See everything across your applications and workloads
- Enable intelligent policy management for dynamic workloads with a single source of truth

Enable Effective Microsegmentation and Zero Trust
- Reduce the attack surface across east-west traffic using Palo Alto Networks firewalls and Illumio software
- Automate policy definition, testing/modeling, provisioning, and enforcement for effective workload segmentation

Automate Dynamic Security for Workloads
- Streamline PAN-OS policy changes across Dynamic Address Groups (DAG)
- Reduce complexity by pushing workload telemetry (IPs, Labels, etc.) from Illumio PCE into Panorama and Palo Alto Networks NGFWs

Integration Diagram
Illumio-Palo Alto Networks DAG Updater is an integration tool that makes API calls to Illumio’s PCE to gather information about workloads and registers them on Palo Alto Networks Panorama (1) as well as physical and virtual Palo Alto Networks NGFWs, including PA-7000 Series, PA-5200 Series, PA-3200 Series, and VM-Series (2).

Before You Begin

Dependencies
- Palo Alto Networks
  - Refer to the Integration Details Table for the supported versions of PAN-OS
  - Separate admin account has been setup for XML API access
- Illumio Policy Computer Engine (PCE)
  - Refer to the Integration Details Table for the supported versions of PCE
  - User account with role Ruleset Viewer (PCE running 20.1.x) or role Limited Ruleset Manager (PCE running 19.3.x, 19.1.x, and 18.2.x)
- Illumio-Palo Alto Networks DAG Updater
  - Latest stable release of Ruby
  - Permission to install Ruby gems

Requirements for a Successful Integration
- Palo Alto Networks
  - Create Dynamic Address Groups (DAG) with matching criteria based on labels created on Illumio Policy Computer Engine
  - Create policy using DAG
- Illumio Policy Computer Engine (PCE)
  - Create unique labels on Illumio PCE
- Illumio-Palo Alto Networks DAG Updater
  - Install on a workload that can make API calls
- Illumio-PCE
  - Palo Alto Networks Panorama or NGFWs depending on your configuration
  - Schedule via a cron job at a frequency determined by your business needs
A membership to Dynamic Address Groups (DAG) can be updated on Palo Alto Networks Panorama as well as physical and virtual Palo Alto Networks NGFWs, including PA-7000 Series, PA-5200 Series, PA-3200 Series, and VM-Series. Configure an implementation (Palo Alto Networks Panorama or NGFWs) that works for your business needs.

Palo Alto Networks Panorama Configuration
1. Generate API key using the admin account created for XML API access by making a GET or POST request to Palo Alto Networks Panorama by passing administrative credentials and type=keygen ²

Below is a screenshot generating an API key by making a GET request to Palo Alto Networks Panorama

![API Key Generation Screenshot]

2. Add a User-ID agent on each Palo Alto NGFW connected to Palo Alto Networks Panorama³
   a. Log in to the Palo Alto Networks NGFW
   b. Devices -> User Identification -> Add
   c. Name: Enter a descriptive name (up to 31 characters) for the User-ID agent
   d. Add an Agent Using: Select how the firewall identifies the User-ID agent or redistribution point
   e. Serial Number: Select the Palo Alto Networks Panorama management server that redistributes user mappings to the firewall

Below is an example where User-ID Agent identifies the redistribution point using Serial Number

![User-ID Agent Configuration]

Palo Alto Networks NGFW Configuration
1. Generate an API key using the admin account created for XML API access by making a GET or POST request to Palo Alto Networks NGFWs by passing administrative credentials and type=keygen ²

Below is a screenshot generating an API key by making a GET request to Palo Alto Networks NGFWs

![API Key Generation Screenshot]

Partner Product Configuration

Illumio’s PCE
1. On PCE running 20.1.x, create a user with the role of Ruleset Viewer ⁴ with the appropriate scope. Follow steps below to assign the role and scope.
   a. Log in to the PCE: Visit Role-Based Access -> Scopes and select Add
b. Choose scope: Choose appropriate Application, Environment, and Location values from the drop-down menu
c. Add principals: Choose the user from the drop-down menu
d. Select role: Select Ruleset Viewer

Below is a screenshot of a user with the role of Ruleset Viewer limited in scope to the IOT Application in the Development Environment across All Locations

2. On PCE running 19.3.x, 19.1.x, and 18.2.x, create a user with the role of Limited Ruleset Manager with the appropriate scope. Follow steps below to assign the role and scope.
   a. Log in to the PCE: Visit Role-Based Access -> Scopes and select Add
   b. Choose scope: Choose appropriate Application, Environment, and Location values from the drop-down menu
   c. Add principals: Choose the user from the drop-down menu
   d. Select role: Select Limited Ruleset Manager

Below is screenshot of a user with the role of Limited Ruleset Manager limited in scope to the Ordering Application in the Development Environment across All Locations

3. Below are steps to generate API keys on PCE 20.1.x using the Web Console
a. Log in to the PCE: Visit the User menu -> My API Keys and select Add

b. Provide a Name and Description for the API Key and click Save

![Create API Key form]

C. Click Download Credentials to download the credentials as a text file. Make sure you have saved the credential information before clicking Close. You’ll need Authentication Username and Secret.

![API Key Created]

Illumio-Palo Alto Networks DAG Updater
The integration tool is written in Ruby and has been tested on latest Ruby versions 2.5.8, 2.6.2, and 2.6.6. Ruby can be installed on UNIX-like operating systems, macOS, and Windows. Package managers or third-party tools can be used to install and manage Ruby. Different installation methods are available at https://www.ruby-lang.org/en/documentation/installation/.

Below are steps to install Ruby 2.6.6 on CentOS 7.6.x using Rbenv. Steps below require a user with sudo privileges and yum installed.

Skip to step 6 if you already have the latest stable version of Ruby installed.

To find the version of Ruby, issue the command ruby -v

Example 1: Ruby installed
```
$:.illumio-panw>ruby -v
ruby 2.6.6p146 (2020-03-31 revision 67876) [x86_64-linux]
$:.illumio-panw>
```

Example 2: Ruby not installed
```
$:.illumio-panw>ruby -v
-bash: ruby: command not found
$:.illumio-panw>
```

To find the version of CentOS, issue the command cat /etc/redhat-releases or rpm -qf /etc/redhat-release

1. Rbenv is a lightweight Ruby version management utility we'll use to install ruby 2.6.6. Install dependencies using yum by issuing the following command:

```
sudo yum install -y git-core zlib zlib-devel gcc-c++ patch readline readline-devel libyaml-devel libffi-devel openssl-devel make bzip2 autoconf automake libtool bison curl sqlite-devel
```

```
$:.illumio-panw>sudo yum install -y git-core zlib zlib-devel gcc-c++ patch readline readline-devel libyaml-devel libffi-devel openssl-devel make bzip2 autoconf automake libtool bison curl sqlite-devel
Loaded plugins: fastestmirror
Determining fastest mirrors
* base: d36watk0698307.cloudfront.net
* extras: d36watk0698307.cloudfront.net
* updates: d36watk0698307.cloudfront.net
base                                                                                           1 3.6 kB  00:00:00
extras                                                                                         1 2.9 kB  00:00:00
illumio                                                                                1 1.5 kB  00:00:00
updates                                                                                       1 2.9 kB  00:00:00
(2/4): base/7/x86_64/group_gz                                                                     153 kB  00:00:00
(2/4): extras/7/x86_64/primary_db                                                                205 kB  00:00:00
(3/4): updates/7/x86_64/primary_db                                                               30 MB  00:00:00
(4/4): base/7/x86_64/primary_db                                                                6.1 MB  00:00:01
Package zlib-1.2.7-18.el7.x86_64 already installed and latest version
Resolving Dependencies
---> Running transaction check
---> Package autoconf.noarch 0:2.69-11.el7 will be installed
---> Processing Dependency: perl => 5.006 for package: autoconf-2.69-11.el7.noarch
---> Processing Dependency: m4 => 1.4.14 for package: autoconf-2.69-11.el7.noarch
---> Processing Dependency: perl(warnings) for package: autoconf-2.69-11.el7.noarch
---> Processing Dependency: perl(vargs) for package: autoconf-2.69-11.el7.noarch
---> Processing Dependency: perl(strict) for package: autoconf-2.69-11.el7.noarch
---> Processing Dependency: perl(constant) for package: autoconf-2.69-11.el7.noarch
2. Install rbenv and ruby-build using curl by cloning repositories from GitHub to ~/.rbenv by issuing the following command:

```
curl -L https://github.com/rbenv/rbenv-installer/raw/master/bin/rbenv-installer | bash -
```

3. Add rbenv to PATH in ~/.bashrc by issuing the following commands:

```
echo 'export PATH="/home/centos/rbenv/bin:$PATH"' >> ~/.bashrc
echo 'eval "$(rbenv init -)"' >> ~/.bashrc
source ~/.bashrc
```

4. Install Ruby 2.6.6 using rbenv by issuing the following command:

```
rbenv install 2.6.6
```
5. Set Ruby 2.6.6 as the default Ruby version by issuing the following command:

```
rbenv global 2.6.6
```

6. Install bundler by issuing the following command:

```
gem install bundler
```

7. Login to Illumio Support Portal and click on Tools. Click on Illumio-Palo Alto Networks DAG Updater. Download the integration tool.
8. Extract the integration tool into a folder by issuing the following command:

```
unzip integration_tool.zip
cd integration_tool
```

9. Install the needed Ruby gems by issuing the following command:

```
bundle install
```
10. Set the environment variables listed below. If you are configuring using Palo Alto Networks NGFWs, set `PANORAMA_URL` with the firewall URL and `PANORAMA_KEY` with the API key generated by the firewall.

- **PCE_URL**  
  #example: https://mypce.test.io
- **PCE_ORG_ID**  
  #example: 1
- **PCE_API_KEY_ID**  
  #example: api_12345
- **PCE_API_KEY_SECRET**  
  #
- **PANORAMA_URL**  
  #example: https://mypanorama.test.io
- **PANORAMA_KEY**  
  #

11. Get help options by issuing the following command:

   **On UNIX-like operating systems & macOS**
   ```bash
   bundle exec ./illumio_panw_dag_updater.rb --help
   ```
12. List all changes without making any changes by issuing the following command:

**On UNIX-like operating systems & macOS**

```
bundle exec illumio_panw_dag_updater.rb --sync --dry-run
```

Below is a screenshot of new IP addresses getting registered on a test instance with an invalid certificate:

---

**Known Limitations**

- Workload IP addresses and labels on the PCE (authoritative source) are used to dynamically register on PAN-OS
- Tags created on PAN-OS don't expire

**Troubleshooting**
1. Where can I download Illumio-Palo Alto Networks DAG Updater?
Illumio-Palo Alto Networks DAG Updater is currently available for Illumio customers and partners via Illumio’s Support portal.

2. Can Illumio-Palo Alto Networks DAG Updater be configured with Palo Alto Networks NGFWs?
Yes. Illumio-Palo Alto Networks DAG Updater can be configured with Palo Alto Networks Panorama as well as physical and virtual Palo Alto Networks NGFWs, including PA-7000 Series, PA-5200 Series, PA-3200 Series, and VM-Series.

3. Can I test without making any changes?
Yes. Use option --dry-run.

4. Valid certificates are not installed on my test instance. Can I run the integration tool?
Yes. Use option --insecure.

5. How can I get support?
Illumio customers and partners can browse Illumio’s Support portal knowledge base and submit a ticket. Support is limited to Illumio API calls and excludes Palo Alto Networks configuration or functionality. Support does not include help in deploying or using the integration tool itself.

References
4. https://docs.illumio.com/asp/20.1/Content/Guides/pce-administration/access-configuration/role-based-access-control.html
5. https://docs.illumio.com/asp/20.1/API-Reference/index.html#create-an-api-key
7. https://support.illumio.com

Palo Alto Networks Technology Partner Program Integration Guide Template, version 1.1: January 15, 2020